

Amendments To The Claims

1. (Previously Presented) A method for securing contents of one or more data storage devices within a computer capable of storing a security password for unlocking and locking the data storage devices and of supporting one or more security features, the method comprising:

reading from each of the data storage devices within the computer a data storage device identifier, the data storage device identifier indicating whether the data storage device supports the security features and whether the data storage device is locked or unlocked;

determining from the data storage device identifier whether the data storage device supports the security features and is locked;

in response to determining that the data storage device supports the security features and is locked, determining whether the data storage device is returning from a powered off state, a hardware reset, or a sleep state;

in response to the data storage device being locked and returning from a powered off state or a hardware reset, determining whether a backup password may be used to unlock the data storage device;

in response to determining that a backup password may be used, determining whether a request to enter a backup password has been received;

in response to receiving a request to enter a backup password, receiving from a user the backup password for unlocking the data storage device and unlocking the data storage device, allowing access to data stored on the data storage device;

in response to determining that the data storage device is locked and returning from a powered off state or a hardware reset and that the backup password may not be used or a request to enter the backup password has not been received, receiving from the user a password for unlocking the data storage device;

in response to receiving the password, determining whether the received password is the security password;

in response to the received password being the security password, unlocking the data storage device and thereby allowing access to data stored on the data storage device;

in response to determining that the data storage device is locked and returning from a sleep state, determining whether the data storage device was unlocked prior to the sleep state; and

in response to determining that the data storage device was unlocked prior to the sleep state, retrieving the security password from the memory and utilizing the security password to unlock the data storage device.

2. (Previously Presented) The method of claim 1, wherein the method is implemented during a power on test procedure of the computer hosting the data storage devices.

3. (Previously Presented) The method of claim 1, further comprising:
in response to the received password not being the security password, determining whether limited access should be provided to each locked data storage device;

in response to determining that limited access should be provided, setting a bit corresponding to each locked data storage device to exclude the locked data storage device from detection verification during a power on test procedure; and

in response to determining that limited access should not be provided to each locked data storage device, isolating each locked data storage device from the operating system.

4. (Original) The method of claim 3, wherein limited access comprises prohibiting reading from or writing to the locked data storage device.

5. (Original) The method of claim 1, wherein the data storage devices are locked upon experiencing a powered off state, a sleep state, or a hardware reset, and wherein the method further comprises:

in response to the received password being the security password, determining whether a data storage device returning from a sleep state should be unlocked without requiring a user to enter a password; and

in response to determining that the data storage device should be unlocked without requiring a user to enter a password, storing the security password within a memory located outside the data storage device.

6. (Canceled)

7. (Previously Presented) The method of claim 1, wherein the security password is stored within the memory in an encrypted format.

8. (Canceled)

9. (Original) The method of claim 1, further comprising:

in response to determining that the data storage device is unlocked, determining whether a security password has been enabled; and

in response to determining that the data storage device is unlocked and that no security password is enabled for the data storage device, disabling, until a next power cycle, the security features that enable security passwords.

10. (Canceled)

11. (Previously Presented) The method of claim 1, further comprising:

in response to the received password being the backup password, determining whether a maximum security is supported by the security features; and

in response to the received password being the backup password and the maximum security being supported, erasing the data storage device before unlocking the data storage device.

12. (Original) The method of claim 1, wherein a password entry attempt counter is set for a maximum number of entry attempts allowed, further comprising:

in response to determining that the password is not the security password, determining whether the password entry attempt counter is equal to zero;

in response to the password entry attempt counter being greater than zero, decrementing the password entry attempt counter by one and again receiving a password from a user; and

in response to the password entry attempt counter equaling zero, prohibiting additional password entries until a next power cycle and displaying a message that the data storage device remains locked.

13. (Original) The method of claim 1, further comprising executing a setup utility within the basic input/output system operative to control one or more functions for manipulating at least one of a security password and a backup password for a data storage device supporting the security features wherein the functions are accessed by one of entering the security password when prompted by the setup utility and selecting the data storage device in the setup utility when said data storage device is unlocked.

14. (Canceled)

15. (Currently Amended) A computer storage medium comprising computer executable instructions which, when executed by a computer, cause the computer to:

read from each of the data storage devices within the computer a data storage device identifier, the data storage device identifier indicating whether the data storage device supports the security features and whether the data storage device is locked or unlocked;

determine from the data storage device identifier whether the data storage device supports the security features and is locked;

in response to determining that the data storage device supports the security features and is locked, determine whether the data storage device is returning from a powered off state, a hardware reset, or a sleep state;

in response to the data storage device being locked and returning from a powered off state or a hardware reset, determine whether a backup password may be used to unlock the data storage device;

in response to determining that a backup password may be used, determine whether a request to enter a backup password has been received;

in response to receiving a request to enter a backup password, receive from a user the backup password for unlocking the data storage device and unlock the data storage device, allowing access to data stored on the data storage device;

in response to determining that the data storage device is locked and returning from a powered off state or a hardware reset and that the backup password may not be used or a request to enter the backup password has not been received, receive from the user a password for unlocking the data storage device;

in response to receiving the password, determine whether the received password is the security password;

in response to the received password being the security password, unlock the data storage device ~~[[allow]]~~ allowing access to data stored on the data storage device;

in response to determining that the data storage device is locked and returning from a sleep state, determine whether the data storage device was unlocked prior to the sleep state; and

in response to determining that the data storage device was unlocked prior to the sleep state, retrieve the security password from the memory and utilize the security password to unlock the data storage device.

16. – 21. (Canceled)